AO 106 (Rev. 04/10) Application for a Search Warrant EC/JMR

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The digital devices and other items listed in Attachment A obtained from on or about the person of Terrael Alls at 875 E. Main Street in Newark, Ohio and currently in the custody of Ohio Organized Crime Investigations or Columbus Police.

Case No. 2:23-mj-228

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1591(a)(1) and (b)	Sex Trafficking by Means of Force, Fraud, or Coercion

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

HSI-TFO
Applicant's signature

HSI TFO Aaron Dennis
Printed name and title

Sworn to before me and signed in my presence.

Date: April 4, 2023

City and state: Columbus, Ohio

Kimberly A. Johnson
United States Magistrate Judge

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**Case No.** 2:23-mj-228
	)	
The digital devices as listed in Attachment A and other items seized also listed in Attachment A that were obtained from on or about the person of Terrael ALLS at 875 E. Main Street Newark, Ohio and which are currently held in the secure custody of the Ohio Organized Crime Investigations Commission or the Columbus Division of Police.	)	**Magistrate Judge**
	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Aaron Dennis, Task Force Agent, United States Department of Homeland Security Investigations (HSI), being duly sworn, depose and state that:

INTRODUCTION

1. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

2. I am a Columbus Ohio Police Officer (Columbus Police Department) currently assigned as a Task Force Officer (TFO) with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI) and The Central Ohio Human Trafficking Task Force (COHTTF). The Columbus Division of Police (CPD) has employed me since 1999. My primary responsibilities as a TFO are to investigate Human Trafficking crimes. During my tenure as a Columbus Police Officer/Detective/Task Force Agent, I have worked multiple investigations regarding Narcotics, Prostitution and Human Trafficking offenses.

3. I am a Columbus Ohio Police Officer (Columbus Police Department) currently assigned as a Task Force Officer (TFO) with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI) and The Central Ohio Human

Trafficking Task Force (COHTTF). The Columbus Division of Police (CPD) has employed me since 1999. My primary responsibilities as a TFO are to investigate Human Trafficking crimes. During my tenure as a Columbus Police Officer/Detective/Task Force Agent, I have worked multiple investigations regarding Narcotics, Prostitution and Human Trafficking offenses.

4. I also have specialized training in the area of Human Trafficking, Pimp Controlled Prostitution, Organized Prostitution, Child Prostitution Rings, Narcotics Trafficking and Money Laundering. I have participated in the execution of search warrants and arrests related to the above-referenced offenses. By virtue of my experience and training, your affiant is familiar with money laundering techniques utilized by individuals involved in illegal activities, such a narcotics and human trafficking. Throughout this affidavit, reference to "investigators" specifically refers to criminal investigators.

5. I have participated in several drug trafficking, money laundering, and organized crime investigations that have resulted in the arrest of numerous members of several different domestic drug trafficking organizations as well as the seizure of currency, assets, and controlled substance related to these investigations. Some of these investigations used judicially authorized electronic surveillance as an investigative technique and I have participated in investigations in support of those judicially authorized electronic surveillance operations. Additionally, I have testified on numerous occasions in grand jury proceedings, procedural hearings, and in criminal trials related to the prosecution of individuals involved in sex trafficking offenses.

6. Through instruction, training, and participation in investigations, I have become familiar with the manner and methods by which narcotics traffickers and sex traffickers conduct their illegal business and the language and terms that are used to disguise conversations about their illegal activities. Moreover, narcotics traffickers and sex traffickers frequently use telephone communications to further their illegal activities by, among other things, remaining in constant communication with one another, either verbally or via text messaging.

7. I am also aware that drug traffickers and sex trafficking organizations utilize texting applications to generate multiple phone numbers, at no cost, to communicate. The texting applications can aide to protect trafficker's identities as well. I am also aware that drug traffickers and sex traffickers often utilize more than one communication device at one time in order to facilitate their drug illegal activities.

PURPOSE OF THE AFFIDAVIT

8. The facts and statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies, information gathered from the service of administrative subpoenas; the results of a cell-site search warrant; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training and background as a Detective and TFO. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have not omitted any facts that would negate probable cause. I have set forth only the facts that I believe are necessary to establish probable cause for a search warrant for the content of four digital media devices that were seized from on or about the person of Terrael **ALLS** on March 31, 2023 at the location of 875 E. Main Street in Newark, Ohio and are currently held in a secure location at the Ohio Organized Crime Investigations Commission or Columbus Division of Police (herein after referred to as the **SUBJECT DEVICES**) and any relevant papers, notes, documents, records or other items of evidentiary value also seized from on or about the person of Terrael **ALLS.**

9. The **SUBJECT DEVICES** and additional documents to be searched are more particularly described in **Attachment A**, for the items specified in **Attachment B**, which items constitute instrumentalities, fruits, and evidence of violations of Title 18 United States Code §§ 1591 and 1594 (Sex Trafficking by Force, Fraud or Coercion and Conspiracy to Commit Sex Trafficking). I am requesting authority to forensically examine the entirety of the **SUBJECT DEVICES**, wherein the items specified in **Attachment B** may be found, and to seize all items listed in **Attachment B** as instrumentalities, fruits, and evidence of crime.

APPLICABLE STATUTES AND DEFINITIONS

10. Title 18, United States Code § 1591 makes it a federal crime for any person, in or affecting interstate or foreign commerce to recruit, entice, harbor, transport, provide, obtain, advertise, maintain, patronize or solicit, by any means, a person, knowing, or in reckless disregard

of the fact that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act. Section 1594 of the same title prohibits attempts or conspiracies to engage in such acts.

11. Pursuant to Title 18, United States Code, Section 1591(e) (3) the term "commercial sex act" is defined as "any sex act, on account of which anything of value is given to or received by any person."

12. The term "computer"[1] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

13. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

14. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

15. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

---

[1]The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

16. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES, MOBILE APPLICATIONS, AND THE INTERNET

17. I know from my training and experience that computer hardware, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

18. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

19. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

20. Digital devices are also capable of sending and receiving messages. Messages can be received or sent on digital devices in a variety of manner, including, but not limited to, e-mail,

texting (including "SMS" and "MMS" messaging), and application messaging (including, but not limited to, Facebook Messenger, Snapchat, and WhatsApp).

21. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses and other information both in computer data format and in written record format.

22. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

23. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with

more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

24. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

25. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in **Attachment B**.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

26. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

A. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the

stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

B. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

27. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU) as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

PROBABLE CAUSE

28. On February 1, 2022, the Central Ohio Human Trafficking Task Force (COHTTF) received an email tip from an emergency operator with the Columbus Division of Police (CPD). The tip referenced a call that had been received from a female (herein after referred to as Witness #1) that had traveled to the Columbus area over the prior weekend. Witness #1 indicated she had been a guest at the Red Roof Inn located at 5001 Renner Road in Columbus, OH 43228 and, while there, was approached by an unknown male who handed her a business card and told her to call him. Witness #1 noted the card was for advertising a modeling agency/business but had concerns there was a possible nexus to human trafficking and wanted to report it to CPD.

29. On February 3, 2022, COHTTF Investigators contacted Witness #1 who confirmed the above tip, explaining she was approached by a male, who offered her the business card and

said he was looking for new models. After the male handed Witness #1 the business card, he walked off. Witness #1 informed law enforcement the business card had "***Elite Diamond Studios***" on the front, along with the phone number (740) 542-1103. The back of the business card also listed the following Gmail address: elitediamond44@gmail.com.

30. Further inquiry via subpoenaed phone records revealed the subscriber's name for the (740) 542-1103 phone number was a female who law enforcement later identified as a victim in this investigation (and who is hereinafter referred to as Victim #1). Through further open-source searches, investigators learned the same (740) 542-1103 phone number was assigned to a CashApp account named "$elitediamondstu" and sex escort advertisements.

31. A subpoena was issued for call records for the (740) 542-1103 number and a review of the returns revealed telephone number (614) 230-4805 exchanged approximately 76 calls/texts with (740) 542-1103 between December 11, 2021 and January 31, 2022. The (614) 230-4805 telephone number was found to be attributed to an individual by the name of **Terrael ALLS** (DOB: 11/07/1994) via a search of law enforcement databases. **ALLS** had also utilized the same phone number to make a call to CPD in February of 2021. The (614) 230-4805 phone number was also linked to several sex escort advertisements and a male black pictured in one of the advertisements and matched the description of **ALLS.**

32. Investigators learned a sex trafficking lead had been received by the Delaware County Sheriff's Office and **ALLS**, who went by the nickname "Rell," had been identified as the possible target subject. On March 29, 2022, an interview was conducted with the source of the information, herein after referred to as Witness #2, while he/she was incarcerated in the Delaware County Jail. Witness #2 informed Delaware County law enforcement he/she was familiar with both Victim #1 and **ALLS** and that **ALLS** was trafficking women.

33. On November 4, 2022, COHTTF Investigators re-interviewed Witness #2, who was still incarcerated. Witness #2 confirmed he/she was familiar with **ALLS** and provided information mostly pertaining to Victim #1, confirming Victim #1 was physically harmed by **ALLS** and coerced with drugs by **ALLS**. Witness #2 stated he/she saw injuries on Victim #1, including marks on her arms and bruises on her shoulders. Witness #2 recalled having a disagreement with **ALLS** about Victim #1 and **ALLS** told him/her not to threaten "the merchandise," referring to Victim #1.

34. Further investigation into **ALLS** revealed in April 2022, Victim #1 was arrested at Red Roof Inn in Dublin, Ohio on an outstanding warrant. **ALLS** was on scene at the time. Upon her arrest, Victim #1 disclosed to police officers that **ALLS** was her pimp and that he recruits women under the guise of modeling for him as a photographer. She further reported **ALLS** limits her movements, gives the women he recruits fentanyl and that she had never engaged in prostitution until **ALLS.**

35. Victim #1 consented to a search and extraction of her cellphone and agreed to speak further with investigators. In summary, Victim #1 explained she was introduced to **ALLS**, whom she identified by name and photograph, and he introduced her to prostitution/escorting. Victim #1 stated **ALLS** got her hooked back on drugs again, specifically fentanyl and methamphetamine. Victim #1 reported **ALLS** would post ads for prostitution and pornographic content, including images and videos on multiple escort sites. Victim #1 reported **ALLS** would try to make $1,000 a day and **ALLS** received all the proceeds in the seven (7) months she worked with him. Victim #1 recalled having a debt she owed to **ALLS** and noted he would keep track of that debt. Victim #1 noted in response to investigators questions that she never worked enough or made enough to get a day off. Your affiant knows from training and experience that traffickers often use debt, typically fictional debt, as a means of controlling victims.

36. Victim #1 stated **ALLS** posed as the female whom the customer was planning to meet with. **ALLS** would set up the "dates," a term your affiant knows is often used to describe the exchange of sexual acts for money or other things of value. Victim #1 explained that a customer would text the phone number from her advertisement to set up a date and/or ask for videos containing sexual content. Law enforcement obtained records for **ALLS'** Facebook accounts and recovered videos of Victim #1 engaged in masturbation and sex acts, including sex acts with **ALLS.**

37. Victim #1 reported the clients would use CashApp to pay for the content and that the videos were sent either through text messages or email. Victim #1 reported **ALLS** had multiple CashApp names including DiscordC and EliteDiamondStudios, which were connected to a CashApp card. Investigators obtained records from CashApp for both Victim #1 and **ALLS**, which confirmed Victim #1 had used the app to transfer $11,677 to **ALLS** over an approximate 5-month period of time. The records from CashApp also contained a request for "$100 or blood" from

ALLS to Victim #1, followed by another note in which **ALLS** threatened Victim #1 by indicating "I'm looking at you."

38. Victim #1 stated she is fearful of **ALLS**, noting that he frequently physically abused her, carried a firearm, threatened to pistol-whip her, and had fired a gun near her head in the past. During the investigation, your affiant learned that in or about February 2022, **ALLS** had rented a hotel room and the hotel cleaning crew had located a firearm in that room. Hotel management at the hotel had photographed the firearm. Law enforcement obtained that photograph and Victim #1 positively identified the firearm in the photo as the one **ALLS** carried and threatened her with. Investigators were also able to locate a photo of **ALLS** posing with the same firearm on his social media.

39. Victim #1 reported **ALLS** gave her whatever drugs she needed to stay "well," which your affiant knows to be a means of providing another individual with enough drugs to that they do not suffer the effects of drug withdrawal. Victim #1 further explained all the money she received from the clients went back to **ALLS** and, in return, he would give her drugs to keep her well. Victim #1 reported both she and **ALLS** used fentanyl and meth (in that order) so she could stay awake to see more clients.

40. Victim #1 also informed investigators **ALLS** receives his mail at his grandmother's home. Further investigation revealed that specific address was tied to numerous email accounts used by **ALLS** to promote sex services on corresponding sex escort advertisements. Victim #1 also reported **ALLS** has eight (8) different emails that correspond with eight (8) different TextNow numbers, which were each assigned women working with **ALLS** at any given time[2].

41. Investigators performed a forensic extraction of Victim #1's phone. This extraction revealed photographs of bruises to Victim #1's face and thigh and messages from **ALLS** regarding the sexual activity for hire and her monetary debt to him

[2] Throughout the course of the investigation, your affiant served legal process on TextNow and identified a total of nine different TextNow telephone numbers attributed to **ALLS**, the majority of which corroborated the solicitation of Victim #1 in acts of prostitution.

42. As the investigation continued, law enforcement identified an additional victim, hereinafter referred to as Victim #7 for purposes of this affidavit[3]. On January 31, 2023, investigators interviewed Victim #7 who reported she was familiar with **ALLS** and he contacted her in 2022 via Facebook with the pretense of modeling in "adult entertainment." Victim #7 said she knew **ALLS** as "Ace Finesse" or "Ace" and positively identified **ALLS** in a photograph. Victim #7 reported she did not initially realize the business involved prostitution and she had never engaged in prostitution prior to meeting **ALLS.** Victim #7 explained she did eventually engage in prostitution under the direction of **ALLS** and he kept all the proceeds, typically collected via Cash App. Victim #7 reported **ALLS** set up most of the dates and did most of the communication with customers. Victim #7 noted most of **ALLS'** customers seemed to be regular clientele.

43. Victim #7 was aware **ALLS** used online platforms to advertise her and identified herself in a sex escort advertisement created by **ALLS.** Victim #7 explained she had been "clean" prior to meeting up with **ALLS**, who then provided her with "meth" and "weed." Victim #7 explained she never paid **ALLS** for the drugs, he instead just took it out of the proceeds she would make. Victim #7 noted **ALLS** would tell her she would "need to push content" because he "didn't buy this for nothing," referring to the drugs. Victim #7 stated **ALLS** would use the drugs against her, knowing she would want to get high, to get what he wanted.

44. Victim #7 explained the night before she left **ALLS,** he threatened physical violence, pushed her around and "got a little rough with me." Victim #7 further explained **ALLS** became mad about money and told her if she didn't come up with "$100 for the room rent" she was going to be kicked out and "no longer a partner" with him. **ALLS** also told Victim #7 "If you don't give me my drugs and shit I'm going to beat the fuck out of you." These threats eventually led Victim #7 to call police for assistance who responded to the scene. Officers were wearing body cameras which captured **ALLS** in the background and Victim #7 in a state of duress. Your affiant obtained the CPD incident report that was generated as a result of this call. Officers noted in the report Victim #7 was "scared" and made allegations of sex trafficking.

---

[3] Numerous victims of **ALLS** were identified through the course of the investigation. For purposes of this criminal complaint, only two are mentioned: Victim #1 and Victim #7.

45. Further investigation revealed escort advertisements depicting Victim #7 had been posted on the website Megapersonals. TextNow legal process and search warrant returns also indicated that on or about April 27, 2022, Victim #7 was referred to as a new model working for **ALLS** and given a unique nickname by him. In addition, search returns from Facebook and Snapchat revealed Victim #7 created pornographic content with **ALLS** or for **ALLS.** CashApp returns that were obtained throughout the course of the investigation also revealed **ALLS** received the money from that content in addition to the money Victim #7 made from the sex acts she engaged in with others.

46. On or about March 29, 2023, a federal criminal complaint and arrest warrant were issued for **ALLS** for Sex Trafficking by Means of Force, Threats, Fraud, or Coercion in violation of 18 U.S.C. § 1591 (a)(1) and (b).

47. On March 31, 2023, **ALLS** was placed in custody on the aforementioned arrest warrant. At the time of his arrest, **ALLS** was noted as the front seat passenger of a 2005 Lincoln Town Car, with Ohio registration #JZT7545. The registered owner of the vehicle was the driver.

48. When **ALLS** exited the passenger side of the vehicle upon his arrest, left in the area he was seated in was a Targus backpack that was black in color. The driver of the vehicle indicated that the bag belonged to **ALLS** and that he had been carrying for approximately two days prior. At the time the backpack was seized, **ALLS** denied ownership of the backpack. The driver of the vehicle gave officers consent to search the vehicle and the backpack, also denying again that the backpack belonged to her.

49. The backpack seized from on or about the person of **ALLS** property was opened pursuant to a search incident to his arrest. A list of items contained within the backpack was made pursuant to inventory protocol and processes. The following digital media devices were contained within the backpack: one Silver iPhone – IMEI: 35923906749329; one Purple Motorola cellphone and charger; one Green Gateway Laptop – Model: GWTC116-2BL; and one Black and Gray ONN Tablet – S/N: 1483GR220445235 (the **SUBJECT DEVICES**). In addition, the following other noteworthy items were documented by law enforcement: one blue notebook, one black and white composition notebook; and one wallet with additional unknown contents.

50. All of the **SUBJECT DEVICES** listed in Attachment A were seized from on or about the person of Terrael **ALLS** and specifically, the black backpack that was recovered in the front

passenger seat where he had been seated. All of those devices, in addition to the other items of interest as outlined above, were subsequently transported to the Ohio Organized Crime Investigations Commission or the Columbus Division of Police and have remained in law enforcement custody since the time they were seized.

51. Based on the information that had been gathered to date, combined with your affiant's belief that Terrael **ALLS** is involved with the trafficking of women for sex by means of force, fraud, and coercion as described above, your affiant believes that there is probable cause that the **SUBJECT DEVICES** and other items recovered from the backpack contain evidence of **ALLS** sex trafficking and exploitation activities and that further evidence of his activities will be contained within the **SUBJECT DEVICES** or the additional items inventoried from his backpack.

SEARCH METHODOLOGY TO BE EMPLOYED FOR DIGITAL MEDIA DEVICES

52. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **SUBJECT DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:

A. Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment B;
B. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in Attachment B;
C. Surveying various files, directories and the individual files they contain;
D. Opening files in order to determine their contents;
E. Scanning storage areas;
F. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

G. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

53. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

AUTHORIZATION REQUEST

54. Based on all the forgoing information, there is probable cause to believe that violations of Title 18 United States Code §§ 1591 and 1594 (Sex Trafficking by Force, Fraud or Coercion and Conspiracy to Commit Sex Trafficking) have been committed and that evidence, fruits and instrumentalities of these offenses will be found within the **SUBJECT DEVICES** listed in **Attachment A**, which is incorporated herein by reference, or within the papers, notes, documents, and records also seized from on or about the person of Terrael **ALLS.** Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT DEVICES** described in **Attachment A**, as well as the items outlined above and below, and the seizure of the items described in **Attachment B**.

HSI-TFO

Aaron Dennis
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 4th day of April, 2023.

Kimberly A. Johnson
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF ITEMS TO BE SEARCHED

The devices to be searched are listed as follows:

1. Silver iPhone – IMEI: 35923906749329
2. Purple Motorola cellphone and charger
3. Green Gateway Laptop – Model: GWTC116-2BL
4. Black and Gray ONN Tablet – S/N: 1483GR220445235

The relevant papers, notes, documents, records or other items of evidentiary value are listed as follows:

1. One blue notebook
2. One black and white composition notebook
3. One wallet with additional unknown contents.

This warrant authorizes the forensic examination of the **SUBJECT DEVICES** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
INFORMATION TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18 United States Code §§ 1591 and 1594 (Sex Trafficking by Force, Fraud or Coercion and Conspiracy to Commit Sex Trafficking), including but not limited too all electronically stored or recorded/handwritten data on the **SUBJECT DEVICES** or other items as described in **Attachment A** and also:

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs.
2. List of customers and related identifying information;
3. Types, amounts, and prices of drugs as well as dates, places, and amounts of specific transactions;
4. Any information related to source of drugs (including names, addresses, phone numbers, or any other identifying information);
5. Any information related to travel or schedule, particularly for the purpose of obtaining quantities of narcotic drugs or scheduling sex in exchange for money;
6. All bank records, checks, credit card bills, account information, and other financial records;
7. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
8. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs, and electronic messages,) pertaining to the charges listed above.
9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an

Internet Service Provider or Electronic Communications Service, including any social media accounts.

10. Any and all messages, emails, voicemails, texting applications, text messaging, or social media communications pertaining to prostitution or sex trafficking, including, but not limited to, hotel/motel reservations, car services, posting of prostitution advertisements, and communications regarding the scheduling of dates or payment for sexual services.
11. Any and all lists of names, telephone numbers, and addresses related to the operation of sex trafficking/prostitution services and drug trafficking.
12. Any and all records, files, or documents showing dominion, ownership, custody, or control over the **SUBJECT DEVICES** or other items seized as outlined in **Attachment A** including evidence showing user attrition at the time the things described in the warrant were created, edited, deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history and in addition, the following:
    a. logs, phonebooks, saved usernames and passwords, documents, and browsing history, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the **SUBJECT DEVICES**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the **SUBJECT DEVICES** were accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
    e. evidence indicating the user's state of mind as it relates to the crime under investigation;
    f. evidence of the attachment to the **SUBJECT DEVICES** of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICES**;

h. evidence of the times the **SUBJECT DEVICES** were used; and

i. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICES**.

13. Any other forms of storage media and other system components to include mobile applications, global positioning system history, memo and notes, and all indicia, documents and records of co-conspirators, and any other individuals or business with whom a financial relationship exists and the authority to put any electronically stored data and/or items in human viewable form.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement, including the FBI, may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.